BPC Market Pilot Certificate Policy

Version 1.0
April 5, 2022

Contents

Version History

Revision Date	Version	Change Description	Editor Name
2/23/2022	0.1	Initial creation	Britta Holland
4/5/2022	1.0	Steering Committee Approval	Britta Holland

1. Introduction

1.1. Scope

This document defines the policy for the management and use of certificates in waves one and two of the BPC market pilot.

1.2. Conformance

The keywords ‘MUST’, ‘MUST NOT’, ‘REQUIRED’, ‘SHALL’, ‘SHALL NOT’, ‘SHOULD’, ‘SHOULD NOT’, ‘RECOMMENDED’, ‘MAY’, and ‘OPTIONAL’ in this specification are to be interpreted as described in RFC2119 and RFC 8174 when, and only when, they appear in all capitals, as shown here.

1.3. Terms and Definitions

For the purpose of this specification, all terms shall have the definitions defined in section 2.3 of the E-invoice Exchange Framework – Approach to Managing a Federated Registry Services Model in a Four-Corner Network report found here: https://businesspaymentscoalition.org/wp-content/uploads/bpc-e-delivery-network-validation-exercise-2020.pdf

1.4. Disclaimers and Copyright

> Views expressed here are not necessarily those of, and should not be attributed to, any particular BPC participant or organization. They are not intended to provide business or legal advice, nor are they intended to promote or advocate a specific action, payment strategy, or product. Readers should consult with their own business and legal advisors.

2. Certificate Policies and Management

2.1. Summary

Certificates are used to control and validate access in the BPC e-invoice exchange framework. Service providers in the BPC network are required to manage two different types of electronic certificates:

- TLS/SSL certificates, used on transport level to provide a standard solution for securing server authentication and message confidentiality.
- BPC market pilot certificates, used on application level to ensure that only authorized and approved service providers are operating within the BPC network.

The TLS/SSL Certificates are not provided by the BPC and MUST be issued by third party Certificate Authorities as specified in section 3.

The BPC market pilot certificates are issued by a Certificate Authority approved by the BPC.

2.2. Registration Authority Role

All service providers accepted into the BPC market pilot MUST receive a certificate from an approved Certificate Authority. The process for accepting service providers into the market pilot is out of scope for this document.

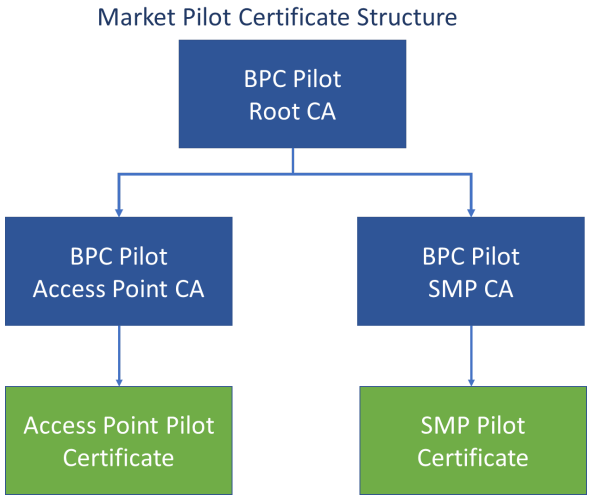
2.3. Certificate Authority Role

During waves one and two of the market pilot, the Certificate Authority role MUST be fulfilled by a BPC market pilot participant. It is the responsibility of the Certificate Authority to issue certificates to market pilot participants based on the policies and processes outlined in this document.

2.4. Certificate Requirements

2.4.1. Trusted Root Certificates

Each BPC approved CA MUST have exactly one root certificate (Trusted Root Certificate). All intermediate certificates issued by the CA MUST be signed using the private key of the CA's Trusted Root Certificate. The CA MUST make its Trusted Root Certificate available to all service providers in the network, as illustrated below.



All service providers in the BPC MUST trust all certificates as outlined in section 2.4.2.1 below. Service providers in the BPC MUST NOT trust certificates that are not derived from a Trusted Root Certificate.

For the BPC market pilot, the Trusted Root Certificates MUST NOT be valid *after* June 30, 2023. The key length of a Trusted Root Certificate MUST be exactly 2048 bits. The signing algorithm of a Trusted Root Certificate MUST be SHA256 with RSA encryption.

2.4.2. Service Provider Certificates

2.4.2.1. Intermediate certificates and service provider types

A BPC approved CA MUST generate exactly one intermediate certificate per service provider type defined by the BPC, i.e., one intermediate certificate for Access Point service providers, one intermediate certificate for SMP service providers, as well as one intermediate certificate for each additional service provider type defined by the BPC market pilot. The CA MUST make these intermediate certificates available to all service providers in the network.

The CA MUST NOT use the BPC intended intermediate certificates for any certificate signing outside of the BPC network.

A CA MUST issue a Service Provider Certificate to each service provider who requests it, as specified in section 2.5. The Service Provider Certificate MUST be signed using the private key of the intermediate certificate corresponding to the service provider type, i.e., an Access Point certificate MUST be signed using the CA's intermediate certificate for Access Points, an SMP certificate MUST be signed using the CA's intermediate certificate for SMPs, and so on.

A CA MUST NOT sign a Service Provider Certificate using an intermediate certificate intended for a different service provider type.

Service providers MUST only trust certificates signed using an intermediate certificate corresponding to the use of the certificate. I.e., service providers MUST NOT trust communication from an Access Point using a certificate issued for use by an SMP service, etc.

2.4.2.2. Identifying service providers

Each service provider in the BPC network is identified by a Business Identifier, as specified in the BPC Policy for Using Identifiers. The Subject CN field of a Service Provider Certificate MUST be identical to the Business Identifier of the service provider it is issued for.

Before issuing a Service Provider Certificate, a CA MUST validate that the Subject CN field of the certificate signing request (CSR) is identical to the Business Identifier that the service provider has communicated to the BPC market pilot.

A service provider MUST NOT make use of certificates with a Subject CN value that is different from their Business Identifier.

The business identifier in the Subject CN value of the certificate MUST be formatted as follows:

```
{identifier scheme}::{participant ID}
```

2.4.2.3. Service Provider Certificate requirements

A certificate issued to a BPC market pilot service provider MUST conform to the following requirements:

- The key length of the Service Provider Certificate MUST be exactly 2048 bits.
- The signing algorithm of the Service Provider Certificate MUST be SHA256 with RSA Encryption.
- The Service Provider Certificate MUST have the following key usage extensions:
    - Digital signature
    - Key encipherment
- The certificate MUST be valid from the date of issue and MUST NOT be valid after June 30, 2023.
- The Subject CN field of the certificate MUST be identical to the service provider's Business Identifier, as specified in section 2.4.2.2.

No other certificate attributes are required.

2.5. Certificate Issuing Process

The Certificate Authority issues certificates using the following process:

- Access Point and SMP providers MUST create a Certificate Signing Request (CSR) that conforms to requirements in section 2.4 and send to the Certificate Authority
- The Certificate Authority signs the certificate with the corresponding intermediate certificate key and returns it to the service provider.

2.6. Certificate Revocation

Certificate revocation is out of scope for waves one and two.

3. SSL Certificates

All HTTP services where applicable must use HTTPS. SSL/TLS certificates and configurations used for HTTPs must adhere all of the following requirements:

- The certificate MUST be issued (directly or indirectly) by a Certificate Authority whose certificate is contained in the latest version of the “Server Authentication (SSL/TLS) Root Certificates” list of the Mozilla Common CA Database.
- TLS MUST be configured to include the certificate chain in the TLS handshake.
- The key length of the certificate MUST be at least 2048 bits.
- The signing algorithm of the certificate MUST be SHA256 with RSA Encryption.
- The TLS configuration MUST support TLS protocol version 1.2 and MAY support higher versions.

4. References

- Mozilla Common CA DB

  https://www.ccadb.org

- TLS Root CA list:

  https://ccadb-public.secure.force.com/mozilla/IncludedRootsPEMTxt?TrustBitsInclude=Websites

- Mozilla Network Security Services

  https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS

- List of preloaded CA certificates of NSS
  https://wiki.mozilla.org/CA/Included_Certificates